学校编码：10384
学号：19020111152533
分类号_____密级_____
UDC_____

厦门大学

硕 士 学 位 论 文

基于身份的无双线性对多代理签名方案

An ID-based Multi-Proxy Signature Scheme without Bilinear Pairings

吴 媛 媛

指导教师姓名： 曾 吉 文 教授
专 业 名 称： 基础数学
论文提交日期： 2014 年 月
论文答辩时间： 2014 年 月
学位授予日期： 2014 年 月

答辩委员会主席：_____
评 阅 人：_____

2014 年 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘要

在现实世界里, 人们经常需要将自己的某些权力委托给可靠的代理人, 让代理人代表本人去行使这些权力. 在这些可以委托的权力中包括人们的签名权. 委托签名权的传统方法是使用印章, 因为印章可以在人们之间灵活地传递. 数字签名是手写签名的电子模拟, 但是数字签名不能提供代理功能. 因此, 作为普通的数字签名的变种, 提出了代理签名的概念. 代理签名方案允许一个代理签名者代替一个原始签名者签署信息.多代理签名方案是代理签名体制的延伸. 在多代理签名方案中, 一个原始签名者可以授权一个代理组作为他的代理机构, 要求只有代理签名组中所有签名者的共同合作才可以代替原始签名者产生代理签名. 许多使用双线性对的基于身份的多代理签名方案已被提出, 但是在椭圆曲线中双线性对的计算量大约是普通数量乘法的二十几倍.

为了减少签名的运行时间及长度, 在这篇文章里, 我们提出了一种无需双线性对的基于身份的多代理签名方案. 我们也给出了在随机谕示模型下, 其抵抗可适应性选择消息攻击的安全性证明. 由于节省了运行时间, 我们的方案在效率上有很大的提升, 具有更强的应用性.

关键词：数字签名; 基于身份; 多代理签名; 双线性对; 椭圆曲线.

Abstract

In real world, people often need to delegate certain powers to the reliable agent, then the agent on behalf of himself can exercise these powers. In these powers delegated, there exist the sign powers of the people. The traditional way of delegating sign powers is to use the seal, because the seal can be flexibly transfered between people. Digital signature is an electronic simulation of handwritten signature, but digital signature can't offer agency functions. So as a variation of ordinary digital signature scheme, the concept of proxy signature is proposed. Proxy signature scheme enables a proxy signer to sign messages on behalf of the original signer. Multi-proxy signature is an extension of the basic proxy signature primitive. In a multi-proxy signature scheme, an original signer could authorize a proxy group as his proxy agent. Then only the cooperation of all the signers in the proxy group can generate the proxy signatures on behalf of the original signer. Plenty of identity-based multi-proxy signature (IBMPS) schemes using bilinear pairings have been proposed. But the relative computation cost of the pairing is approximately more than twenty times of the scalar multiplication over elliptic cure group.

In order to save the running time and the size of the signature, in this paper, we propose an IBMPS scheme without bilinear pairings. We also prove the security of our scheme against adaptive chosen message attack under random oracle model. Wth the running time being saved greatly, our scheme is more applicable than the previous related schemes for practical applications.

Key Words: Digital Signature; Identity-based; Multi-proxy signature; Bilinear pairings; Elliptic cure.

目 录

CONTENTS

第一章　绪 论

1.1 研究背景

随着计算机软硬件及网络技术的飞速发展, 各种网络服务已经渗透到人们生产生活的各个领域. 这的确给人们的活动带来了巨大的便利和好处, 同时却也带来了前所未有的威胁. 网络攻击、网络病毒在不断地变种、升级, 严重威胁企业及个人信息安全. 网络信息安全正随着全球信息化步伐的加快而显得日趋重要. 信息安全主要体现在：数据的机密性, 保护数据内容免于非授权泄露；数据的完整性, 防止数据遭受篡改, 保证收到的数据确实授权实体所发出的数据；认证, 保证通信实体是它所声称的实体；不可抵赖性, 防止整个或部分通信过程中, 任意通信实体进行否认的行为.

密码学是对与信息安全各方面有关的数学技术的研究, 其基本目的是使得两个在不安全信道中通信的人, 以一种他们的敌手不能明白和理解通信内容的方式进行通信. 密码学有着悠久的历史, 早在4000年前, 埃及人就开始使用密码；在20世纪两次世界大战中密码学也扮演着关键的角色.

现代密码学形成于20世纪70年代, 有两个重要标志：一是1977年美国国家标准和技术研究所（NIST）采纳和公布了公用数据加密标准（DES, Data Encryption Standard）；二是公钥密码体制的诞生. 现代密码学的应用已不再局限于军事、政治和外交, 其商用价值和社会价值已得到了广泛的重视.

1.1.1 基于身份的密码体制

在公钥密码体制中, 密钥都是成对出现的, 每一对密钥由一个公钥和一个私钥组成. 私钥由拥有者自己保存, 而公钥要公之于众. 为了公钥体系的广泛应用, 一个基础性的问题就是公钥的分发和管理. 公钥本身没有标记, 仅从公钥本身无法判断用户的身份. 因此, 公钥密码体制使用公钥证书的方法在公钥和用户身份间建立联系. 但在对证书的管理和支持及结构上的配置是传统公钥密码体制比较复杂的问题之一.

1984年, Shamir[1]第一次提出了基于身份的密码体制. 其主要特点是, 系统中不需要证书, 可以使用用户的标识如姓名、IP地址、电子邮件地址等作为公钥. 用户的私钥通过一个被称作私钥生成器PKG(Private Key Generator)的可信第

三方进行计算得到. 基于身份的数字签名方案在1984年Shamir[1]就已得到. 然而直到2001年, Boneh和Franklin[2]利用椭圆曲线的双线性对才得到Shamir意义上的基于身份的加密方案(Identity-Based Encryption, IBE), 该方案是建立在随机谕示模型下的. 在此之前, 一个基于身份的更加传统的加密方案曾被Cocks[3]提出, 但效率更低. 目前, 基于身份的方案包括基于身份的加密体制、签名体制、可鉴别身份的加密和签密体制、密钥协商体制、门限密码体制、前向安全密码体制、强前向安全密码体制等.

1.1.2 多代理签名体制

Mambo et al.[4]在1996年第一次提出了代理签名体制的概念. 在代理签名方案中, 有两个参与者：原始签名者和代理签名者. 原始签名者授权他的签名权给代理签名者, 代理签名者代替原始签名者产生有效的签名. 自从此概念被提出, 产生了许多代理签名方案[5][6][7][8][9]. 代理签名方案被应用在许多方面, 如电子商务、电子政务、电子现金、电子投票及移动代理等. 所以该概念一经提出便引起了国内外专家学者的广泛关注. 而且许多代理签名体制的变种也被提出, 如门限代理签名[10], 代理盲签名[11], 代理环签名, 一次代理签名, 多代理签名[12][13], 代理多签名[14][15]及多代理多签名[16]等. 而在实际的应用中, 人们对代理的需要也不尽相同.

代理签名人的权力过于集中, 可能会出现权利滥用的情况. 于是人们想分散代理签名人的权利, 通过一组代理签名人来签名, 只有满足一定数量的代理签名人合作完成签名, 才能完全代表原始签名人的签名. 实现的方案称为门限代理签名; 如果要求这组获得授权的代理签名人都得签名才能代表原始签名人时,该方案称为多代理签名方案. 该方案是由Hwang和Shi[12]第一次提出的. 在多代理签名方案中,一个原始签名者可以授权一个代理组作为代理机构, 要求只有代理组中的所有代理签名者的共同合作才能代替原始签名者产生代理签名. 它可以应用于如下场景：假设一个公司的老板需要去外地出差, 在此期间, 他将会收到许多重要的文件必须由他签署, 有一些可能还需立即回复, 为解决此问题, 在他出差前, 他可以授权他的签名权给每个部门经理, 然后此文件必须由老板授权的部门经理共同合作签署. 解决此问题的方法就是使用一个多代理签名方案.

使用双线性对, 已提出了许多新的基于身份的签名方案[17][18][19], 基于身份的代理签名(IBPS) 方案[5][6][7][8][9]及多代理签名方案[13]. 上述所有的IBPS方案都是非常实用的, 但是它们都是基于双线性对的. 而双线性对被认为